UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,584	04/16/2001	Christopher E. Mitchell	MS1-775US	7869

22801	7590	09/15/2006	EXAMINER

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.usplo.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/836,584
Filing Date: April 16, 2001
Appellant(s): MITCHELL ET AL.

William J. Breen, III
For Appellant

**Supplemental
EXAMINER'S ANSWER**

This is in response to the appeal brief filed June 15, 2006 appealing from the Office

action mailed June 29, 2005.

(1) Real Party in Interest

The statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

Claims 1-47 are rejected under 35 U.S.C. 102(b) as being anticipated by Baker et al (US 5,678, 041).

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Baker et al   US 5,678,041   October 14, 1997

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-47 are rejected under 35 U.S.C. 102(b) as being anticipated by Baker et al (US 5,678, 041).

    a.   _Referring to claim 1:_

        i.   Baker teaches:

        (1)   associating a first entity with a second entity in a first device **[i.e., as shown in Figure 1, the system includes public network 100, network resources 101-105, and user site 106. Particular users at user site 106**

gain access to public network 100 via user terminals 107, 108 and 109. Each of these user terminals is linked by local area network ("LAN") 110 to processor 111 within proxy server 112 (column 3, lines 60-65)]; and

(2)   selectively providing information about the association of the first and second entities to a second device as directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device [i.e., relational database 114 stores a list of user terminal identification codes and the various user clearances reflective of the ratings of network resources that each user terminal should be allowed to retrieve from public network 100. It will be understood that the invention could be modified so that the list of user clearances associated with a given user terminal identification code serves as a restrictive list (i.e.; that user is not allowed to retrieve network resources having that rating). This restrictive listing functionality could be readily facilitated by reprogramming processor 111. In addition, the invention could be modified so that the identification codes recognized by processor 111 and stored in relational database 114 are user specific, as opposed to user terminal specific. In other words, the system of Figure 1 could be modified so that a given individual using a terminal is identified to the system by a personal password or other identifying code. Access or denial of the transmission of particular URLs is effected by the system as a function of that person's identity, regardless of the particular user terminal they may be utilizing (column 5, lines 45-65)].

b.   *Referring to claim 2:*

i.   Baker further teaches:

(1)   wherein the first entity and the second entity are selected from a group of entities that includes users, organizations, companies, devices, computers, servers, computer programs, and applications [i.e., as shown in Figure 1, the system includes public network 100, network resources 101-105, and user site 106 (column 3, lines 60-61)].

c.   *Referring to claims 3-8, 33-36, 39, 41-44:*

      i.   These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

    d.   *Referring to claim 9:*

      i.   Baker further teaches:

        (1)   wherein the first entity is a parent/guardian of the second entity **[i.e., Baker's invention overcomes the deficiencies of prior schemes for regulating network database access by providing a system and method that allows one or more network administrators/managers, that is "parent/guardian", to rate particular information and/or services. This rating is then employed to restrict specific system users from accessing the information/services via certain public or otherwise uncontrolled databases (i.e., the WWW and the Internet) (column 3, lines 7-15)].**

    e.   *Referring to claim 10:*

      i.   Baker further teaches:

        (1)   wherein the first device includes a network server that is configured to act as an authentication server **[i.e., proxy server 112 provides a connection from processor 111 to public network 100 via firewall 113. Requests from user terminals 107-109 for access to network resources (101-105) through public network 100 are submitted to processor 111 within proxy server 112. In this particular embodiment of the invention, the submitted requests are assumed to be in the form of URLs. When URLs are submitted to a proxy server (that is "authentication server"), the particular requesting user terminal is identified to the proxy server by an identification header attached to the URL. (column 3, line 65 through column 4, line 9)].**

    f.   *Referring to claim 11:*

      i.   Baker further teaches:

        (1)   wherein the second device includes a network server that is configured to act as an affiliated server associated with the authentication server **[i.e., within the system of Figure 1, URLs designated as URL.sub.101, URL.sub.102, URL.sub.103, URL.sub.104 and URL.sub.105, represent requests for**

information from network resources 101, 102, 103, 104 and 105 (these are "affiliate servers"), respectively (column 4, lines 12-16)].

     g.   *Referring to claims 12, 32:*

         i.   These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

     h.   *Referring to claims 13, 38:*

         i.   These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

     i.   *Referring to claims 14-19:*

         i.   These claims have limitations that is similar to those of claim 12, thus they are rejected with the same rationale applied against claim 12 above.

     j.   *Referring to claims 20, 29, 45:*

         i.   These claims have limitations that is similar to those of claim 9, thus they are rejected with the same rationale applied against claim 9 above.

     k.   *Referring to claims 21,30, 47:*

         i.   These claims have limitations that is similar to those of claim 10, thus they are rejected with the same rationale applied against claim 10 above.

     l.   *Referring to claims 22, 31, 46:*

         i.   These claims have limitations that is similar to those of claim 11, thus they are rejected with the same rationale applied against claim 11 above.

     m.   *Referring to claim 23:*

         i.   Baker teaches:

         (1)   memory having information associating a first user of the apparatus with a second user of the apparatus **[i.e., as shown in Figure 1, the system includes public network 100, network resources 101-105, and user site 106. Particular users at user site 106 gain access to public network 100 via user terminals 107, 108 and 109. Each of these user terminals is linked by local area network ("LAN") 110 to processor 111 within proxy server 112 (column 3, lines 60-65). The above described system may also be modified so that URLs are**

identified as being in a rating category within the memory structure of a relational database (column 5, line 66 through column 6, line 1)]; and

        (2)   logic operatively coupled to the memory and configured to respond to inputs from the first user by selectively outputting the information about the association of the first user and the second user, without requiring the second user to be operatively signed-in to the apparatus **[i.e., for example, if a system manager wished to modify relational database 302 from user terminal 108, he or she would enter a password identifying themselves as an authorized system manager. The password is received by processor 111 and compared with the contents of manager ID memory listing 304. If the received manager ID password corresponds to one stored in listing 304, then user terminal 108 is identified as a manager terminal (as indicated by ID.sub.108 being stored within listing 304). Modifications to the contents of relational database 302 may then be effected from that user terminal. When all modifications have been completed, the manager logs off and user terminal 108 returns to standard user terminal status (i.e., ID.sub.108 is cleared from listing 304) (column 7, lines 3-16 and claim 1 (2))].**

    n.   *Referring to claim 24:*

    i.   This claim has limitations that is similar to those of claim 23, thus it is rejected with the same rationale applied against claim 23 above.

    o.   *Referring to claims 25-28:*

    i.   These claims have limitations that is similar to those of claim 23, thus they are rejected with the same rationale applied against claim 23 above.

    p.   *Referring to claims 37, 40:*

    i.   These claims have limitations that is similar to those of claim 23, thus they are rejected with the same rationale applied against claim 23 above.

(10) Response to Arguments

Regarding to the Appellant's arguments on anticipation by Baker. Appellant states that it is unclear what the Examiner is asserting for a first entity, a second entity, or for an association between first and second entities (see Appellant's Brief, page 14).

Since, the claimed language broadly recites, especially, the term "association", in which examiner interprets as the act of associating or the state of being associated or an organized body of people, users, administrators, etc. who have an interest, activity, or purpose in common. Thus, the limitation of "associating a first entity, i.e., network resources and user sites, with a second entity, i.e., user terminals, in a first device" is met on **(column 3, lines 60-65 of Baker).** For further clarification, Baker also discloses as shown in Figure 3, processor 111 can be programmed to allow resource categorization information (listing 300) and/or user/user terminal clearance information (listing 301) within relational database 302 to be modified only by a specific dedicated management terminal 303. Restricting ability to "write" new information into relational database 302 to management terminal 303 minimizes opportunities for database tampering. Alternately, the system can also be configured to permit database modification to be performed from any one of user terminals 107, 108 or 109. To protect against corruption of the contents of relational database 302, authorization for altering the contents of relational database 302 from a user terminal is controlled via use of a manager identifier. For example, if a system manager wished to modify relational database 302 from user terminal 108, he or she would enter a password identifying themselves as an authorized system manager. The password is received by the processor 111 and compared with the contents of manager ID memory listing 304. If the received manager ID password corresponds to one stored in listing 304, then user terminal 108 is identified as a manager terminal (as indicated by ID.sub.108 being stored within listing 304). Modifications to the contents of relational database 302 may then be effected from that user terminal. When all modifications have been completed, the manager logs off and user terminal 108 returns to standard user terminal status (i.e., ID.sub.108 is cleared from listing 304) (column 6, lines 57-67 and columm 7, lines 1-16 of Baker). Thus, Baker teaches the claimed associating a first entity with a second entity in a first device.

Appellant further argues that Baker fails to describe "selectively providing information about the association of the first and second entities to a second device as directed by the first entity" or "without requiring the second entity to be operatively

associated with either the first or second device." Baker does disclose this kind of relationship between the manager and the users as mentioned in column 6, lines 57-67 and columm 7, lines 1-16 of Baker. Besides, Baker teaches the relational database 114 stores a list of user terminal identification codes and the various user clearances reflective of the ratings of network resources that each user terminal should be allowed to retrieve from public network 100. **The system could also be implemented so that the list of user clearances associated with a given user terminal identification code serves as a restrictive list** (i.e.; that user is not allowed to retrieve network resources having that rating). This restrictive listing functionality could be readily facilitated by reprogramming processor 111. In addition, the invention could be modified so that the identification codes recognized by processor 111 and stored in relational database 114 are user specific, as opposed to user terminal specific. **Baker teaches that the system of Figure 1 could be implemented so that a given individual using a terminal is identified to the system by a personal password or other identifying code. Access or denial of the transmission of particular URLs is effected by the system as a function of that person's identity, regardless of the particular user terminal they may be utilizing** (column 5, lines 45-65 of Baker).

It is therefore shown that the components disclosed by Baker constitute the claimed associating a first entity with a second entity in a first device; and selectively providing information about the association of the first and second entities to a second device as directed by the first entity, without requiring the second entity to be operatively associated with either the first or second device.

Regarding Appellant's arguments to claim 32 that Baker does not disclose, teach, or suggest "a validation code (i.e., identification code) that identifies a first entity and a second entity". Baker teaches this particular limitation as shown in elements 115, 201, 301 (ID 107- ID 109 and manager ID 106) of Figures 1-3. In fact, Baker discloses this identification code associating with users 107-109 through the entire invention. Some fewer examples are shown here: for the system shown in Figure 1, the identification code for user terminal 107 is ID.sub.107, the identification code for user terminal 108 is ID.sub.108, and the identification code for user terminal 109 is

ID.sub.109. In addition, within the system of Figure 1, URLs designated as URL.sub.101, URL.sub.102, URL.sub.103, URL.sub.104 and URL.sub.105, represent requests for information from network resources 101, 102, 103, 104 and 105, respectively. Then upon receipt of an incoming URL, processor 111 is programmed to determine the identity of the requesting user terminal from the URL header. This identification information is then utilized by processor 111 to cross-reference the received URL with information stored in relational database 114. Relational database 114 contains listing 115 which associates each of the user identification codes (ID.sub.107, ID.sub.108 and ID.sub.109) with a user clearance code (user clearances.sub.107, user clearances.sub.108 and user clearances.sub.109, respectively) (column 4, lines 9-25 of Baker). Thus, Baker teaches the claimed validation code that identifies a first entity and a second entity.

Regarding Appellant's arguments to claim 9 that Baker again does not disclose, teach, or suggest "wherein the first entity is a parent/guardian (i.e., administrator - whether network or system, or manager - whether network or system) of the second entity." Baker teaches the claimed limitation as shown in column 5, lines 36-40; and further details in column 6, lines 57-67 and column 7, lines 1-16 of Baker. It is clearly understood that parent/guardian has controlled over the children just like administrator has controlled over the users regardless of the authority level or security level that the administrator has. In fact Baker's invention does teach a system and method for selectively controlling database access by providing a system and method that allows a network administrator or manager to restrict specific system users from accessing information from certain public or otherwise uncontrolled databases (i.e., the WWW and the Internet). The invention employs a relational database to determine access rights, and this database may be readily updated and modified by an administrator. Within this relational database specific resource identifiers (i.e., URLs) are classified as being in a particular access group. The relational database is arranged so that for each user of the system a request for a particular resource will only be passed on from the local network to a server providing a link to the public/uncontrolled database if the resource identifier is in an access group for which the user has been assigned specific
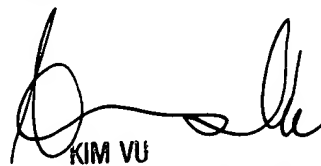
permissions by an administrator (see Baker's abstract). In addition, Baker's invention overcomes the deficiencies of prior schemes for regulating network database access by providing a system and method that allows one or more network administrators/managers to rate particular information and/or services. This rating is then employed to restrict specific system users from accessing the information/services via certain public or otherwise uncontrolled databases (i.e., the WWW and the Internet). The invention in Baker employs a relational database to determine access rights, and store rating information. The rating information database may be readily updated and modified by an administrator/manager. Within this relational database specific resource identifiers (i.e., URLs) are classified as being associated with a particular access rating. The relational database is arranged so that for each user of the system a request for a particular resource will only be passed on from the local network to a server providing a link to the public/uncontrolled database if the resource identifier has an access rating for which the user has been assigned specific permissions by an administrator/manager (column 3, lines 7-27 of Baker). Thus, Baker teaches the first entity is a parent/guardian (i.e., administrator - whether network or system, or manager - whether network or system) of the second entity.

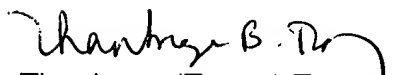For the above reasons, it is believed that the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

Thanhnga (Tanya) Truong
January 6, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees
Kim Vu KV
Hosuk Song HS